Sicurezza Bitcoin

La sicurezza del bitcoin è complicata, perché il bitcoin non è un riferimento astratto ad un valore come può essere il saldo di un conto bancario. Bitcoin è molto più simile all'idea del contante digitale, o all'oro. Probabilmente avrete già sentito l'espressione, "Possession is nine-tenths of the law" ("Il possedere è nove decimi della legge" - detto britannico riferito al sistema legislativo locale per cui chi possiede un bene è considerato legittimo proprietario fino a prova contraria). Con bitcoin si può estremizzare questo concetto, e dire che chi possiede è il legittimo proprietario, punto. La proprietà delle chiavi per sbloccare il bitcoin è equivalente al possesso di denaro contante o di un pezzo di metallo prezioso. Il bitcoin può essere smarrito, perso, rubato, o è possibile accidentalmente versare un importo errato a qualcuno. In ognuno di questi casi, gli utenti non hanno diritto ad alcun ricorso, proprio come se fossero caduti loro dei contanti su un marciapiede pubblico.

Tuttavia, bitcoin ha una capacità che contanti, oro, e conti bancari non hanno. Un portafoglio bitcoin, contenente le chiavi, può essere sottoposto a backup come un qualsiasi file. Può essere conservato in copie multiple, o addirittura stampato su carta in copia fisica. Non è possibile effettuare un "backup" di contanti, oro, o conti bancari. Bitcoin è così diverso da tutto ciò è esistito fino ad ora che si presenta la necessità di concepire la sua sicurezza in modo completamente nuovo.

Principi sulla Sicurezza

Il principio alla base di Bitcoin è la decentralizzazione, la quale ha importanti implicazioni per la sicurezza. Un modello centralizzato, come ad esempio una banca tradizionale o una rete di pagamento, dipende dal controllo degli accessi e dalla sorveglianza volta al tenere ogni possibile minaccia lontano dal sistema. Facendo un paragone, un sistema decentralizzato come bitcoin sposta la responsabilità ed il controllo verso gli utenti. Poiché la sicurezza della rete è basata su prove di transazione piuttosto che sul controllo degli accessi, la rete può essere a modello aperto, e non è necessaria alcuna crittografia per il traffico dei bitcoin.

In una rete di pagamento tradizionale, come ad esempio un sistema di carte di credito, il pagamento è 'open-end' perché contiene l'identificativo privato dell'utente (il numero di carta di credito). Dopo l'addebito iniziale, chiunque abbia accesso all'identificativo privato può "ritirare" denaro ed addebitare somme al proprietario più e più volte. Per questo motivo, la sicurezza della rete di pagamento deve essere garantita da un capo all'altro con crittografia, e deve garantire che nessun intercettatore o intermediario possa compromettere il traffico dei pagamenti, sia nella fase di transito che nell'archiviazione (a riposo). Se un malintenzionato riesce ad accedere al sistema, esso può compromettere transazioni in corso *e* payment token (gettoni di pagamento) che possono essere utilizzati per creare nuove transazioni. Peggio ancora, quando i dati dei clienti sono compromessi, i clienti sono esposti a rischio di furto di identità e devono intervenire per evitare l'utilizzo fraudolento dei conti compromessi.

Il sistema bitcoin è sensibilmente diverso. Una transazione bitcoin autorizza esclusivamente un valore specifico ad un destinatario specifico, e non può essere contraffatta o modificata. La transazione infatti non rivela alcuna informazione privata, come l'identità delle parti, e non può essere utilizzata per autorizzare pagamenti successivi. Pertanto, una rete di pagamento bitcoin non

ha bisogno di essere criptata o protetta da intercettazioni. Anzi, è possibile persino trasmettere le transazioni bitcoin su un canale pubblico aperto, come reti Wi-Fi o Bluetooth, senza alcuna rischio in termini di sicurezza.

Il modello di sicurezza decentralizzato di bitcoin mette molto potere nelle mani degli utenti. Questo potere implica però la responsabilità di mantenere la segretezza delle proprie chiavi. Per la maggior parte degli utenti questo non è semplice, in particolare su dispositivi computerizzati generici come smartphone connessi ad Internet o computer portatili. Anche se il modello decentralizzato impedisce il tipo di compromissione dati che avviene con i sistemi di carte di credito, molti utenti non riescono a mantenere al sicuro le proprie chiavi in maniera adeguata e vengono derubati, uno per uno.

Sviluppare Sistemi Bitcoin Sicuri

Il principio più importante per gli sviluppatori in ambito bitcoin è la decentralizzazione. La maggior parte degli sviluppatori avranno familiarità con i modelli di sicurezza centralizzati, e potrebbero essere tentati di applicare questi modelli ad applicazioni bitcoin, con risultati disastrosi.

La sicurezza di bitcoin si basa sul controllo decentralizzato delle chiavi e sulla convalida indipendente delle transazioni da parte dei miner. Se si vuole mantenere la sicurezza bitcoin, è necessario assicurarsi di rimanere nel modello di sicurezza nato da bitcoin. In sostanza: non prendere possesso del controllo delle chiavi (private) di utenti, e non eseguire transazioni fuori dalla blockchain.

Ad esempio, molti dei primi scambi in bitcoin concentravano tutti i fondi degli utenti in un unico portafoglio "caldo" (chiamato cold wallet ndt) con chiavi memorizzate su un unico server. Tale struttura rimuove il controllo da parte degli utenti e centralizza il controllo delle chiavi in un unico sistema. Molti di questi sistemi sono stati attaccati, con conseguenze disastrose per i loro clienti.

Un altro errore comune è quello di portare le transazioni "off blockchain" (fuori dalla blockchain) tentando in modo errato di ridurre le spese di transazione o di accelerare l’elaborazione delle transazioni. Un sistema "off blockchain" (fuori dalla blockchain) registrerà le operazioni su un libro mastro interno, centralizzato, sincronizzandole solo occasionalmente alla blockchain bitcoin. Questo sistema, ancora una volta, sostituisce al modello di sicurezza bitcoin decentralizzato un modello proprietario e centralizzato. Quando le operazioni sono "off blockchain" (fuori dalla blockchain), i libri mastri centralizzati protetti in maniera non adeguata possono essere falsificati, dirottando fondi ed esaurendo risparmi con operazioni che possono passare del tutto inosservate.

A meno che non si sia disposti ad investire cospicuamente in sicurezza operativa, in livelli multipli di controllo degli accessi ed in verifiche (allo stesso modo delle banche tradizionali) si dovrebbe riflettere molto attentamente prima di portare dei fondi al di fuori del contesto di sicurezza decentralizzato bitcoin. Anche se si è in possesso dei fondi e delle competenze necessarie per realizzare un modello di sicurezza robusto, tale sistema non farebbe altro che replicare il fragile modello di reti finanziarie tradizionali afflitte da furto di identità, corruzione, e appropriazione indebita. Per usufruire del modello unico e decentralizzato di sicurezza bitcoin è necessario evitare la tentazione di produrre architetture centralizzate, il quale modello è sì familiare, ma sovverte la sicurezza di bitcoin nella sua sostanza.

La Radice della Fiducia

L'architettura di sicurezza tradizionale si basa su un concetto chiamato *root of trust*, un nucleo di fiducia utilizzato come base per la sicurezza dell'intero sistema o applicazione. L'architettura di sicurezza si sviluppa intorno alla root of trust come una serie di cerchi concentrici, simili agli strati di una cipolla, estendendo la fiducia dal centro verso l'esterno. Ogni livello si basa sul livello interno più attendibile utilizzando controlli di accesso, firma digitale, crittografia ed altre informazioni primitive di sicurezza. Più i sistemi software diventano complessi, più sono propensi a contenere bug, che li rendono vulnerabili alla compromissione della sicurezza. Come risultato di ciò, più un sistema software diventa complesso, più è difficile proteggerlo. Il concetto di root of trust assicura che la maggior parte della fiducia sia posizionata all'interno della parte meno complessa del sistema, e quindi meno vulnerabile, mentre l'architettura del software più complessa è stratificata intorno ad esso. Questa architettura di sicurezza è ripetuta a scale diverse, in primo luogo stabilendo una root of trust all'interno dell'hardware di un unico sistema, quindi estendendo quella root of trust, attraverso il sistema operativo, a servizi di sistema di livello superiore, ed infine a molti server stratificati in cerchi concentrici in di fiducia che diminuisce andando verso l'esterno.

L'architettura di sicurezza bitcoin è diversa. In bitcoin, il sistema di consenso crea un registro pubblico di fiducia completamente decentralizzato. Una blockchain la cui validità è verificata correttamente utilizza il genesis block (blocco genesi) come root of trust, costruendo una catena di fiducia che si estende fino al blocco attuale. I sistemi bitcoin possono, e devono, utilizzare la blockchain come root of trust. Se si progetta un'applicazione bitcoin complessa, che consiste in servizi su diversi sistemi, è necessario esaminare attentamente l'architettura di sicurezza, in modo da poter verificare dove viene posta la fiducia. In definitiva, l'unica cosa a cui si può dare fiducia esplicitamente è una blockchain la cui validità è verificata completamente. Se nella vostra applicazione viene conferita fiducia, in modo esplicito o implicito, a qualsiasi componente che non sia la blockchain, la si dovrebbe considerare come una potenziale fonte di problemi, dato che introduce vulnerabilità. Un buon metodo per valutare l'architettura di sicurezza della vostra applicazione è quello di considerare ogni singolo componente e valutare un ipotetico scenario in cui tale componente sia completamente compromesso e sotto il controllo di un malintenzionato. Considerare ogni componente della vostra applicazione e, uno alla volta, valutare l'impatto sulla sicurezza complessiva se tale componente fosse compromesso. Se la vostra applicazione non può più essere considerata sicura quando uno o più componenti sono compromessi, ciò mostra una collocazione errata della fiducia in tali componenti. Un'applicazione bitcoin senza vulnerabilità dovrebbe essere vulnerabile solo come compromesso del meccanismo di consenso bitcoin, il che significa che la sua root of trust si basa sulla parte più forte della architettura di sicurezza bitcoin.

I numerosi esempi di exchange bitcoin hackerati, evidenziano l'importanza di questo punto, perché la loro architettura di sicurezza ed il loro design fallisce anche le verifiche più superficiali. Queste implementazioni centralizzate avevano dato fiducia in modo esplicito a numerosi componenti di fuori della blockchain bitcoin, come gli hot wallet, registri database centralizzati, chiavi di crittografia vulnerabili, e altri schemi simili.

Le "Best Practices" sulla Sicurezza livello Utente

Gli esseri umani hanno utilizzato controlli di sicurezza fisici per migliaia di anni. In confronto ciò, in quanto a sicurezza digitale abbiamo meno di 50 anni di esperienza. I sistemi operativi general purpose moderni non sono molto sicuri e non sono particolarmente adatti alla memorizzazione di

denaro digitale. I nostri computer sono costantemente esposti a minacce esterne attraverso connessioni internet sempre on line. Essi gestiscono migliaia di componenti software prodotti da centinaia di sviluppatori diversi, spesso con accesso senza vincoli ai file dell'utente. Un unico componente software malevolo, tra le molte migliaia installati sul computer, può compromettere la tua tastiera e i tuoi file, rubando ogni bitcoin "contenuto" in applicazioni wallet. Il livello di manutenzione del computer necessario per mantenere un computer privo di virus e trojan è attuabile da una piccola minoranza di utenti, in quanto va ben oltre il livello di competenza informatica di un utente medio.

Nonostante decenni di ricerca e progresso nel campo della sicurezza delle informazioni, i beni digitali sono purtroppo ancora vulnerabili a nemici determinati. Persino i sistemi più altamente protetti ad accesso limitato, in società di servizi finanziari, agenzie di intelligence, e industria della difesa, sono spesso violati. Bitcoin crea risorse digitali che hanno un valore intrinseco e possono essere rubati e dirottati a nuovi proprietari immediatamente ed in maniera irrevocabil. Questo crea un incentivo enorme per gli hacker. Fino ad ora, gli hacker hanno dovuto convertire informazioni di identità o token di account—ad esempio carte di credito, e conti bancari—in beni dopo averli violati. Nonostante la difficoltà dei processi di schermaggio e di riciclaggio delle informazioni finanziarie, la quantità di furti che si verificano è sempre crescente. Bitcoin diminuisce questo problema perché non ha bisogno di essere schermato o riciclato; è un valore intrinseco di un bene digitale.

Fortunatamente, bitcoin crea anche gli incentivi per migliorare la sicurezza informatica. Mentre in passato i rischi di compromissione del computer erano vaghi ed indiretti, bitcoin rende questi rischi chiari ed evidenti. Il possesso di bitcoin su computer serve a far meditare l'utente sulla necessità di migliorare la sicurezza del computer. Come diretta conseguenza della proliferazione e dell'aumento di utilizzatori di bitcoin e di altre valute digitali, si è potuta riscontrare un'escalation sia di techniche di hacking che di soluzioni di sicurezza. In parole semplici, gli hacker hanno adesso un obiettivo molto allettante mentre gli utenti hanno un chiaro incentivo per difendersi.

Nel corso degli ultimi tre anni, come risultato diretto dell'aumento di utilizzatori di bitcoin, si è verificato un enorme progresso nel campo della sicurezza delle informazioni nelle forme di criptaggio hardware, salvataggio delle chiavi e wallet fisici (hardware wallet), nella tecnologia multi-signature, e in digital escrow. Nelle sezioni seguenti esamineremo diverse procedure consigliate per la sicurezza utente.

Archiviazione Fisica dei Bitcoin

Dato che la maggior parte degli utenti si trova molto più a suo agio con sicurezza fisica piuttosto che con sicurezza di informazioni, un metodo molto efficace per la protezione dei bitcoin è il convertirli in forma fisica. Le chiavi bitcoin non sono altro che lunghi numeri. Ciò significa che possono essere memorizzate in forma fisica, come ad esempio stampate su carta o incise su una moneta metallica. La sicurezza delle chiavi diventa a quel punto altrettanto semplice quanto il custodire la copia stampata delle chiavi bitcoin. Un set di chiavi bitcoin che viene stampato su carta è chiamato "paper wallet", ed esistono molti strumenti gratuiti che possono essere utilizzati per crearli. Per quanto mi riguarda, custodisco la stragrande maggioranza dei miei bitcoin (99% o più) su dei paper wallet, cifrati con BIP0038, con più copie custodite in casseforti. Custodire bitcoin offline è definito come_cold storage_ ed è una delle tecniche di sicurezza più efficaci. Un sistema cold storage è un sistema in cui le chiavi vengono generate da un sistema offline (non si è mai connesso a Internet) e

memorizzate offline su carta o su supporti digitali, come ad esempio una chiavetta USB.

Wallet Hardware

Con l'avanzare del tempo, la sicurezza bitcoin adotterà in modo sempre crescente la forma di hardware wallet a prova di manomissione. A differenza di uno smartphone o di un computer desktop, un hardware wallet bitcoin ha un solo scopo: custodire i bitcoin in modo sicuro. Senza alcun software general-purpose a rischio di compromissioni e con interfacce limitate, gli hardware wallet sono in grado di offrire un livello quasi infallibile di sicurezza ad utenti non esperti. Prevedo che questi diventeranno il metodo più diffuso di custodire i bitcoin. Per un esempio di hardware wallet, si veda Trezor.

Bilanciamento del Rischio

Anche se la maggior parte degli utenti sono comprensibilmente preoccupati dai furti bitcoin, esiste un rischio ancor maggiore. I file di dati vengono smarriti continuamente. Se questi contengono bitcoin, la perdita può essere ancor più gravosa. Nel tentativo di proteggere i loro portafogli bitcoin, gli utenti devono stare molto attenti a non oltrepassare il limite, rischiando di perdere i propri bitcoin. Nel luglio del 2011, un progetto di sensibilizzazione ed educazione al bitcoin molto conosciuto perse quasi 7000 bitcoin. Cercando di impedire furti, i proprietari implementarono una serie complessa di backup crittografati. Alla fine di ciò, essi persero accidentalmente le chiavi di crittografia, rendendo i backup inutili e perdendo un'intera fortuna. Così come nascondere i soldi seppellendoli nel deserto, se si proteggono i propri bitcoin 'troppo' bene si rischia di non essere in grado di ritrovarli.

Diversificazione del Rischio

Porteresti il tuo intero patrimonio netto in contanti nel tuo portafoglio? Quasi tutti considererebbero una cosa del genere piuttosto spericolata, tuttavia spesso gli utenti bitcoin tengono tutti i loro bitcoin in un unico wallet. Al contrario, gli utenti bitcoin dovrebbero frazionare il rischio suddividendo i propri possedimenti in diversi wallet bitcoin. Gli utenti prudenti manterranno solo una piccola frazione, forse meno del 5%, dei loro bitcoin in un wallet online o mobilewallet, come "spiccioli". Il resto dovrebbe essere diviso su diversi sistemi di deposito, come ad esempio un desktop wallet e offline (cold storage).

Multi-sig e Amministrazione

Ogni volta che una società o un individuo custodisce una grossa quantità di bitcoin, essi dovrebbero considerare la possibilià di utilizzare un indirizzo bitcoin multi-signature. Gli indirizzi multi-signature proteggono i fondi richiedendo più di una firma per effettuare il pagamento. Le chiavi di firma sono conservate in luoghi diversi e sotto il controllo di persone diverse. In un ambiente aziendale, per esempio, le chiavi sono generate in modo indipendente e custodite da diversi dirigenti aziendali, per essere sicuri che nessuno possa compromettere i fondi aziendali da solo. Gli indirizzi multi-signature sono anche in grado di offrire ridondanza, con una persona singola che detiene diverse chiavi custodite in luoghi diversi.

Sopravvivenza

Un’importante considerazione riguardante la sicurezza che viene spesso trascurata è la disponibilità, specialmente nel contesto di incapacità o morte del proprietario delle chiavi. Spesso viene detto agli utenti bitcoin di utilizzare password complesse e di mantenere le loro chiavi al sicuro, non condividendole con nessun altro. Purtroppo, questa pratica rende quasi impossibile per la famiglia dell’utente di recuperare i fondi se l’utente non è più in grado di sbloccarli. Nella maggior parte dei casi, infatti, le famiglie degli utenti bitcoin potrebbero essere completamente all’oscuro dell’esistenza di tali fondi bitcoin.

Se possiedi molti bitcoin, dovresti considerare condividere i dettagli di accesso con un parente fidato o un avvocato. Uno schema di sopravvivenza più complesso potrebbe essere quello di impostare un accesso multi-signature e una pianificazione immobiliare dei beni attraverso un un avvocato specializzato come "digital asset executor."

Conclusioni

Bitcoin è una tecnologia completamente nuova, senza precedenti e relativamente complessa. Man mano che passa il tempo svilupperemo strumenti migliori per la sicurezza e metodologie più semplici da applicare per i non esperti. Per ora, gli utenti di bitcoin possono utilizzare molti dei suggerimenti discussi in questo libro per godere di un’esperienza sicura e senza problemi.